IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: HARALD VATER ET AL

SERIAL NO.: 09/763,621

     FILED: April 26, 2001

     FOR: ACCESS-PROTECTED DATA CARRIER

GROUP ART UNIT: 2134

EXAMINER: C. Colin

ATTY. REFERENCE: VATE3002/BEU

COMMISSIONER OF PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The below identified communication(s) or document(s) is(are) submitted in the above application or proceeding:

☐ Declaration

☐ Priority Document

☐ Formal Drawings

☐ Assignment

☒ **Check - $500**

☐ Application Data Sheet

☒ **Appellant's Brief (in triplicate)**

☒ Please debit or credit **Deposit Account Number 02-0200** for any deficiency or surplus in connection with this communication. A duplicate copy of this sheet is provided for use by the Deposit Account Branch.

☐ Small Entity Status is claimed.

☐

23364
Customer Number

BACON & THOMAS, PLLC
625 SLATERS LANE - FOURTH FLOOR
ALEXANDRIA, VIRGINIA 22314
(703) 683-0500

DATE: __April 3, 2006__

Respectfully submitted,

Benjamin E. Urcia
Attorney for Applicant
Registration Number: 33,805

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re U.S. Patent Application of:	)	Group Art Unit: 2134
	)	
Harald VATER *et al.*	)	Examiner: C. Colin
	)	
Serial Number: 09/763,621	)	*Attorney Docket*: VATE3002beu
	)	
Filed: April 26, 2001	)	Confirmation No.: 8124

For: Access-Protected Data Carrier

APPELLANT'S BRIEF UNDER 37 C.F.R. §1.192

Sir:

This paper is an Appeal Brief in furtherance of the Notice of Appeal filed in this case on February 2, 2006. The fee required under 37 C.F.R. §1.17(f) accompanies this Appeal Brief.

This Brief contains these items under the following headings and in the order set forth below:

I.   Real Party In Interest

The real party in interest is Giesecke & Devrient, GmbH, of Munich, Germany.

II.   Related Appeals And Interferences

There are no related appeals or interferences.

III.   Status of Claims

The status of the claims in this application is:

A.   Status of all the claims

    1.   Claims canceled: None

    2.   Claims withdrawn from consideration: None

    3.   Claims pending: 1-18

    4.   Claims allowed: None

    5.   Claims objected to: None

    6.   Claims rejected: 1-18

B.   Claims on Appeal:

The claims on appeal are: 1-18

IV.   Status of Amendments

No amendments have been submitted subsequent to the rejection mailed November 16, 2005.

V.   Summary of Claimed Subject Matter

The claimed subject matter is a data carrier having a semiconductor chip with a memory and operating program that disguises an operation h and its input x so that, instead of performing

operation h on input x,

performs: disguised operation h_{R1} on disguised input x,

the result of performing disguised operation h_{R1} on disguised input x being the same as performing operation h on input x. The reason for disguising operation h and input x in this manner is to prevent an eavesdropper from revealing operation h by performing a statistical analysis of the signal patterns emitted by the chip during execution of the operating program.

Claim 1 specifically recites that the operation h is disguised *before its execution* to obtain the disguised operation h_{R1} that is a different operation than the operation h. Claim 1 also recites that the disguised operation is executed with disguised input data, and that the result of performing the disguised operation on the disguised data is the same as performing the original, non-disguised operation (*i.e.*, operation h) on the original, non-disguised input data. Finally, claim 1 recites the function of preventing analysis of operation h upon interception of signal patterns generated during execution of the disguised operation. In other words, claim 1 specifically recites at least the following elements:

- operation h disguised to obtain disguised operation h_{R1} **different** from operation h;
- execution of disguised operation on disguised input data;
- result of execution of disguised operation on disguised data **same** as execution of operation h on input data x;
- disguising operation h prevents analysis of h based on signal patterns generated during execution of h_{R1}.

Claim 2 recites that a random number is used during the operation and input data disguising operation. There a number of ways that the random number could be used in disguising operation, but the specification describes use of the "exclusive OR" or XOR operation for this purpose since the XOR operation is irreversible–it is impossible to determine the inputs from the output unless one of the inputs is known.

Claim 3 specifically recites the XOR operation, while claim 4 recites an embodiment in which the disguised operation is stored in advance, and claim 4 recites that two different disguised operation as stored in advance. Claim 6 recites recalculation of the disguised operation before execution, claim 7 recites the feature in which the operation to be disguised is effected by a table, and claim 8 recites the disguising of the input data is effect by combination with at least one random number.

Independent claim 9 recites a variation of the data carrier of claim 1 in which the data output by the disguised operation is different from data that would have been output by the original operation h, but which ca be recovered with the aid of data used to disguise operation h. This claim includes all of the limitations of claim 1, including the following elements:

- operation h disguised to obtain disguised operation h_{R1} **different** from operation h;
- execution of disguised operation on disguised input data;
- disguising operation h prevents analysis of h based on signal patterns generated during execution of h_{R1},

except that the result of disguised operation execution on disguised input data is further disguised relative to the result of original operation h execution on the original input data x.

Dependent claim 10 further recites that one random number is used to disguise the data and two random numbers are used to disguise the operation, while dependent claims 11-13 are identical to claims 3-5 except for their dependency from claim 9, claim 14 adds that random numbers for determining one disguised operation are inverses of random numbers for determining a second disguised operation, claims 15-17 correspond to claims 6-8, and claim 18 adds the additional feature that the operation h is a nonlinear operation with respect to the combination used for disguising the operation h.

In summary, the invention is to not only disguise input data on which operation are performed, which is known in the art, but also to disguise the operations themselves for the purpose of preventing a potential attacker from inferring secret information about the semiconductor chip (*e.g.*, the structure of the chip) by intercepting signal patterns. The invention adds a layer of security to the conventional chip security, protecting only against interception of input data and results, but also of the operations themselves. This is not merely a matter of splitting a known operation such as DES into parts, the two parts being undisguised, so as to enable disguising of input data. In the claimed invention, <u>both</u> the input data and the operations being performed are disguised, providing better protection for both the operations and the input data.

VI.   Grounds of Rejection to be Reviewed on Appeal

The rejection to be reviewed on appeal is a rejection of the subject matter of claims 1-18 as anticipated under 35 USC §102(e) in view of U.S. Patent Publication No. 2001/0053220 (the Kocher publication).

VII.   Argument

Reversal of the rejection under 35 USC §102(e) is respectfully requested on the grounds that the Kocher publication does not disclose or suggest, whether individually or in common with any other reference of record, a data carrier having a semiconductor chip with a memory and operating program that disguises an operation h and its input x in order to obtain a disguised operation h_{R1} *different from operation h* and disguised input data in which:

$$h_{R1}(\text{disguised input data}) = y = h(x)$$

holds true, *i.e.*, in which performing the different operation on the disguised input data has the same effect as performing the original operation on the undisguised input data, as recited in independent claim 1, or in which the result of performing the original operation on the undisguised input data can be determined from the output data with the aid of data used for the disguising the operation, as recited in second independent claim 9.

5

In reply to the argument that the Kocher publication does not teach **disguising** of the operation as well as the input data, the Examiner argues that "*in a broad interpretation, even disguising the input data x into x' and performing an operation y' on the disguised input data x' is considered as performing a different operation y'* which is different than the original operation y performed on x. This argument makes no sense. First, Kocher does perform operation y' on disguised input data x', but rather discloses the original operation y on disguised input data x'. **Second, changing the input data does not, under any interpretation, change the operation itself.** An interpretation of the claim language cannot be so "broad" as to defy logic or contradict the actual meaning of the language. An "operation" is **not** defined by the data input to the operation. Rather, an operation is performed on the data. For example, the operation "+" is the same when the input data is 2 and 3, or 2 and 2. Only the results are different. Similarly, the numerous steps that make up DES are the same irrespective of the input data or the numerical values of the keys (which are also input data).

In addition, on page 3 of the Official Action, the Examiner cites page 2, paragraph 12 of the Kocher publication as teaching disguising of the operation applied to the input data. **However, as was discussed at great length during an interview with the Examiner, this passage merely teaches that DES is an example of an algorithm to which the key splitting technique taught by Kocher may be applied.** It does not teach disguising the DES or any other operation. The exact language paragraph 12 of the Kocher publication is:

> *Although the invention has been described in the context of permuting both keys and messages, each into two sub-parts, those skilled in the art will appreciate that either or both (as well as other secret quantities) could be permuted, into a plurality of parts greater than two. In addition, although the invention has been described with respect to DES, the invention can be applied to and adapted to other cryptographic symmetric algorithms, including without limitation Blowfish, SEAL, IDEA, SHA, RC5, TEA, and other cryptographic algorithms involving operations suitable for application of the techniques of this invention.*

This passage clearly does not teach the claimed operation disguising operation. It does not teach modifying the input data so that the same result is obtained using, for example, Blowfish, as would be obtained by applying DES to unmodified input data. It does not teach that Blowfish is, somehow, a disguised version of DES. To the contrary, this passage merely indicates that there are more than one encryption method, and that the invention of Kocher may be applied using any encryption method, so long as it is symmetric (so that the key can be split and parallel operations performed).

The Examiner also cites page 5, paragraphs 52-53 and page 6, paragraph 65 of Kocher as suggesting "*disguising both the input and the operation using reordering, permutation, and randomization.*" Again, the Examiner has misinterpreted Kocher. Kocher contains no teaching of disguising the input *and the operation*. Paragraph 52 of Kocher describes "key and message update processes" (line 1 of paragraph 52), and not disguising the DES operation applied to the key and message. Paragraph 52 also points out that "*if the key is to be used in future transactions, the input parameters for the key are overwritten in the long-term memory with the updated values. . .*" and that "*the input parameters for the message. . .may be reordered and randomized in a similar fashion as for the key. . .At this point, the key and message have been success fully randomized, so attackers cannot force the device to process the same key repeatedly by introducing power failures or other processing interruptions.*" Furthermore, paragraph 53 makes clear the distinction between the algorithm (operation) applied and disguising of the keys/data:

> *At step 120, the initial permutation (IP),* **which is a part of the standard DES** **algorithm,** *is applied to the input message. Because M1 and M2* **[data, not** **operations]** *are stored in permuted form, the initial permutation* **[part of the** **standard DES algorithm]** *needs to affect the value of M1P{M1} and M2P{M2}.* *Although it is possible for an implementation to modify the data (i.e., M1 and M2),* *it is not necessary. The permutation operation* [*i.e.*, the data disguising operation performed to the input data before application of the DES algorithm] *can be applied* *by manipulating only the permutation tables themselves, by applying the IP to the* *permutation M1P and M2P, e.g. by computing a new M1P=IP{M1P} and a new* *M2P=IP{M2P}. Optionally, additional reordering or randomizing* **of the data** *(as* *was performed at step 110) may be performed as well.*

This passage does not, as alleged by the Examiner, teach disguising of any "operation," but rather simply teaches using different permutations (disguises) for the input data M1 and M2, and application of the "**standard DES operation**." Finally, paragraph 65 mentioned by the Examiner teaches a final permutation of the data M1P and M2P, and not any disguising of the "**standard DES operation**" applied to the data.

Similarly, the Examiner cites page 4, paragraph 46, page 7, paragraph 71, and claims 36-37 of the Kocher publication as teaching that "*both the input and the operations are disguised with the help of XOR as recited in amended claims 3 and 11.*" However, paragraph 46 describes computation of a table using "**standard DES**" with no attempt to disguise that the operation is in fact standard DES, and paragraph 71 describes variation of the invention of Kocher involving storing message bits in 128-bit arrays, manipulation of keys in 64-bit instead of 56-bit form, use of blinding operations other than XOR (which are only disclosed as being applied to data and not operations), use of additional permutation tables (which also are only disclosed as being applied to data, and not operations), and so forth. Neither of these paragraphs teaches any sort of **operation** disguising operation in addition to the data disguising operation.

It appears from the statement on page 3, lines 7-10 of the Official Action that the Examiner has confused manipulating permutation tables of Kocher with disguising of the operation. According to the Examiner, "*For example, the initial permutation (operation) can be applied to the input message, also the permutation can be applied by manipulating the permutation tables themselves,* meaning that the operation is disguised differently than the original before its execution" However, the permutation operations are merely operations that disguise the input data by changing the order of the data. According to the method of Kocher, the data is permuted in order to disguise it, and then the "standard DES operation" is applied." The data is not permuted during execution of the DES

operation, or any other operation, but rather during transfer of the data. This is not the same as the claimed operation disguise.

Instead of performing a disguised operation on disguised input data, Kocher only teaches disguising of the input data by applying **permutation tables** to the original input **data**, and performing the **same operations** on the **permutations** of the input data. The operation performed on the disguised (permuted) input data is the **same DES operation** as would have been performed on the original data, albeit **performed in two parallel operations** on the respective parts of the input data using split parts of the original key. Kocher does not teach disguising of the DES operation in the manner claimed, but only the input data and the DES keys.

More specifically, the method described in the Kocher publication involves enhancing DES encryption by splitting a message M and a key K into permutated message components PM1 and PM2, and permutated key components PK1 and PK2, respectively, such that $PM1 \otimes PM2 = M$ and $PK1 \otimes PK2 = K$ holds (see paragraph [0035] of the Kocher publication). Thereafter, the two message/key pairs (PM1,PK1) and (PM2,PK2) are DES-encrypted separately instead of the standard pair (M,K), so that the resulting ciphertexts can be recombined to obtain the same ciphertext that is obtained when encrypting the original message M with the original K (as explained in paragraph [0036] of the Kocher publication. Thus, it holds that:

$$\underline{DES(PM1,PK1)} \Diamond \underline{DES(PM2,PK2)} = \underline{DES(M,K)}$$

where $\Diamond$ symbolizes the recombination operation. There is no attempt to perform a disguised operation on the input in order to obtain the same output values that would be obtained if the original operation were performed on the original data, but only a splitting of data and keys, which has the effect of disguising the original data. **The Kocher publication does mention various**

9

permutations, **but in each case the permutations are of the input data, and provide an additional layer of input data disguise.** There is absolutely no attempt to disguise the operations performed on the permuted data, which are "**standard DES operations.**"

Because the Kocher publication does not disclose or suggest disguising **both** input data and an operation performed on the input data, resulting in a **different operation** being applied to the **different input data**, it is respectfully submitted that the Kocher publication does not anticipate or suggest the claimed invention, and reversal of the rejection of claims 1 and 9 under 35 USC §102(e) is respectfully requested.

In addition, reversal of the rejection of claims 2-8 and 10-18 is respectfully requested by virtue of their dependence from respective claims 1 and 9, and based on the additional limitations recited therein.

Conclusion

For all of the foregoing reasons, Appellants respectfully submit that the Examiner's final rejections of claims 1-18 under 35 U.S.C. §102(e) are improper and should be reversed by this Honorable Board.

Respectfully submitted,

BACON & THOMAS, PLLC

By: BENJAMIN E. URCIA
        Registration No. 33,805

Date: April 3, 2006

Ser. No. 09/763,621

BACON & THOMAS
625 Slaters Lane, 4th Floor
Alexandria, Virginia 22314

Telephone: (703) 683-0500

S:\Producer\beu\Pending Q...Z\V\VATER 763621\appealbrief.wpd

VIII.   **CLAIMS APPENDIX**

1.   A data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation (h), the execution of the operation (h) requiring input data (x) and the execution of the operation (h) generating output data (y), characterized in that

the operation (h) is disguised before its execution to obtain a disguised operation (h_{R_i}) that is a different operation than the operation (h),

the disguised operation (h_{R_i}) is executed with disguised input data, and

the disguising of the operation (h) and the input data (x) is coordinated such that the execution of the disguised operation (h_{R_i}) with disguised input data yields output data (y) identical with the output data (y) determined upon execution of the operation (h) with input data (x),

whereby disguising operation (h) prevents analysis of said operation (h) and exposure of secret information about said semiconductor chip should a potential attacker intercept signal patterns generated during execution of said disguised operation (h_{R_i}).

2.   A data carrier according to claim 1, characterized in that at least one random number (R_i) enters into the determination of the disguised operation (h_{R_i}) and the disguised input data $(x \otimes R_i)$.

3.   A data carrier according to claim 1, characterized in that the disguised operation (h_{R_i}) is generated from the operation (h) with the aid of XOR operations and the disguised input data is generated from the input data (x) with the aid of XOR operations.

4.   A data carrier according to claim 1, characterized in that the disguised operation (h_{R_i}) is permanently stored in the data carrier in advance.

12

5.   A data carrier according to claim 4, characterized in that at least two disguised operations (h_{R1}, h_{R1}) are permanently stored in the data carrier in advance and one of the stored disguised operations (h_{R1}, h_{R1}) is selected randomly when a disguised operation is to be executed.

6.   A data carrier according to claim 1, characterized in that the disguised operation (h_{R1}) is recalculated before its execution and the at least one random number (R_1) is redetermined for said calculation.

7.   A data carrier according to claim 1, characterized in that the operation (h) is realized by a table stored in the data carrier which establishes an association between the input data (x) and the output data (y).

8.   A data carrier according to claim 7, characterized in that the disguising of the input data (x) contained in the table is effected by combination with the at least one random number (R_1).

9.   A data carrier having a semiconductor chip (5) with at least one memory containing an operating program which is able to execute at least one operation (h), the execution of the operation (h) requiring input data (x) and the execution of the operation (h) generating output data (y), characterized in that

the operation (h) is disguised before its execution,

the disguised operation (h_{R1}) is executed with disguised input data to obtain a disguised operation (h_{R1}) that is a different operation than the operation (h),

the disguising of the operation (h) and the input data (x) is coordinated such that the execution of the disguised operation (h_{R1R2}) with disguised input data yields output data which are disguised relative to the output data (y) determined upon execution of the operation (h) with input data (x), and

the output data (y) can be determined from the disguised output data with the aid of data (R_2)

13

used for disguising the operation (h),

whereby disguising operation (h) prevents analysis of said operation (h) and exposure of secret information about said semiconductor chip should a potential attacker intercept signal patterns generated during execution of said disguised operation (h_{R_1}).

10.   A data carrier according to claim 9, characterized in that at least one random number (R_1) enters into the determination of the disguised input data $(x \otimes R_1)$ and at least two random numbers (R_1, R_2) enter into the determination of the disguised operations (h_{R1R2}).

11.   A data carrier according to claim 9, characterized in that the disguised operation (h_{R1R2}) is generated from the input data (x) with the aid of XOR operations and the disguised input data is generated from the input data (x) with the aid of XOR operations.

12.   A data carrier according to claim 9, characterized in that the disguised operation (h_{R1R2}) is permanently stored in the data carrier in advance.

13.   A data carrier according to claim 12, characterized in that at least two disguised operations $(h_{R1R2}, h_{R1'R2'})$ are permanently stored in the data carrier in advance and one of the stored disguised operations $(h_{R1R2}, h_{R1'R2'})$ is selected randomly when a disguised operation is to be executed.

14.   A data carrier according to claim 13, characterized in that the random numbers (R_1, R_2) for determining the first disguised operation (h_{R1R2}) are inverse to the random numbers (R_1', R_2') for determining the second disguised operation $(h_{R1'R2'})$ with respect to the combination used for determining the disguised operations $(h_{R1R2}, h_{R1'R2'})$.

15.   A data carrier according to claim 9, characterized in that the disguised operation (h_{R1R2}) is

14

recalculated before its execution and the random numbers (R_1, R_2) are redetermined for said calculation.

16.   A data carrier according to claim 9, characterized in that the operation *(h)* is realized by a table stored in the data carrier which establishes an association between the input data *(x)* and the output data *(y)*.

17. - A data carrier according to claim 16, characterized in that the disguising of the input data *(x)* contained in the table is effected by combination with the at least one random number (R_1) and the disguising of the output data *(y)* contained in the table is effected by combination with the at least one further random number (R_2).

18.   A data carrier according to claim 1, characterized in that the operation *(h)* is a nonlinear operation with respect to the combination used for disguising the operation *(h)*.

IX.   EVIDENCE APPENDIX

No evidence is submitted herewith.

X.   RELATED PROCEEDINGS APPENDIX

No related proceedings have occurred, and none are pending.